Cisco Success Network and Telemetry Data

This chapter describes about Cisco Success Network and how to enable it on ASA. It also lists the telemetry data points that are sent to the Security Service Engine(SSE) cloud.

About Cisco Success Network

Cisco Success Network is user-enabled cloud service that establishes a secured connection with the Security Service Exchange (SSE) cloud to stream ASA usage information and statistics. Streaming telemetry provides a mechanism to transmit ASA usage and other details in structured format (JSON) to remote management stations for the following benefits:

- To inform you of extra technical support services and monitoring that are available for your product.
- To help Cisco improve its products.

By default, the Cisco Success Network is enabled on the Firepower 4100/9300 platforms that hosts ASA devices (at the blade level). However, for the telemetry data to be transmitted, you must enable the configuration on FXOS at chassis level (see Cisco Firepower 4100/9300 FXOS CLI Configuration Guide) or enable the Cisco Success Network on the chassis manager (see Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide) ASA allows you to disable the telemetry service at any point in time.

The telemetry data that is collected on your ASA devices includes CPU, memory, disk, bandwidth, and license usage, configured feature list, cluster/failover information, and the alike. Refer Cisco Success Network - Telemetry Data, on page 3.

Supported Platforms and Required Configurations

- Supported on FP9300/4100 platforms with ASA version 9.13.1 or above running on it.
- Requires FXOS version 2.7.1 or above to connect with the cloud.

- The SSE connector on FXOS must be connected to the SSE cloud. This connection is established by enabling and registering the smart license with smart licensing backend. The SSE connector on FXOS is automatically registered to the SSE cloud by registering smart license.
- The Cisco Success Network configuration must be enabled on chassis manager.
- The telemetry configuration must be enabled on ASA.

How Does ASA Telemetry Data Reach the SSE Cloud

Cisco Success Network is supported on Firepower 4100/9300 platforms in ASA 9.13(1) by default. The FXOS service manager sends telemetry request daily to the ASA application running on the platform. The ASA engine, based on the configuration and connectivity status, sends the telemetry data either in standalone mode or cluster mode to FXOS. That is, if the telemetry support is enabled in ASA and SSE connector status is connected, the telemetry thread pulls the needed information from various sources such as system or platform or device APIs, license APIs, CPU APIs, memory APIs, disk APIs, smart call home feature APIs, and so on. However, if the telemetry support is disabled in ASA or the SSE connector status is disconnected, ASA sends a response to FXOS (appAgent) indicating the telemetry configuration status and does not send any telemetry data.

FXOS has only one SSE connector instance running on it. When it gets registered with the SSE cloud, it is considered as one device and SSE infra assigns FXOS with one device ID. Any telemetry report that is sent through the SSE connector is categorized under the same device ID. Therefore, FXOS aggregates the telemetry report from each ASA into a single report. Other contents such as smart license account information are added to the report. FXOS then sends the final report to the SSE cloud. The telemetry data is saved in the SSE data exchange (DEX) and available for the Cisco IT team to use.

Enable or Disable Cisco Success Network

Before you begin

- Enable and register smart license on FXOS.
- Enable telemetry support on FXOS at the chassis level (see Cisco Firepower 4100/9300 FXOS CLI Configuration Guide) or enable the Cisco Success Network on the chassis manager (see Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide).

Procedure

To enable the telemetry service on ASA, in the global configuration mode, enter the following commnad. Use the no form of the command to disable the telemetry service:

[**no**] **service telemetry**

Example:

```
ciscoasa(config)# service telemetry
ciscoasa(config)# no service telemetry
```

What to do next

- You can view the telemetry configuration and activities log or the telemetry data. See View ASA Telemetry Data , on page 3
- To view a sample of telemetry data and the data fields, see Cisco Success Network - Telemetry Data, on page 3

View ASA Telemetry Data

Before you begin

- Enable the telemetry service on ASA. See Enable or Disable Cisco Success Network , on page 2

Procedure

To view the telemetry data on ASA devices of your network, enter the following commnad in the privileged EXEC mode:

show telemetry [**history | last-report | sample**]

Example:

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 3. Telemetry support on the chassis: disabled
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent.
```

Use **history** to view the past 100 events that are related to telemetry configuration and activities; **last-report** to view the latest telemetry data that are sent to FXOS in JSON format, and **sample** to view the instantly generated telemetry data in JSON format.

Cisco Success Network - Telemetry Data

Cisco Success Network is supported on Firepower 4100/9300 platforms by default. The FXOS service manager sends telemetry request daily to the ASA engine running on the platform. The ASA engine, on receiving the request, based on the connectivity status, sends the telemetry data either in standalone mode or cluster mode to FXOS. Following tables provide information on the telemetry data points, its description, and sample values.

Table 1: Device Info

Data Point	Description	Example Value
Device Model	Device model	Cisco Adaptive Security Appliance

Data Point	Description	Example Value
Serial Number	Serial number of the device	FCH183771EZ
System Time	System uptime	11658000
Platform	Hardware	FPR9K-SM-24
Deployment Mode	Deployment type	Native
Security context mode	Single/Multiple	Single

Table 2: Versions Info

Data Point	Description	Example Value
Version Global Variable	ASA version	9.13.1.5
Device Manager Version	Device manager version	7.10.1

Table 3: License Info

Data Point	Description	Example Value
Smart License Global Variable	Activated licenses	regid.2015-01.com.cisco.ASA - SSP-STRONG-ENCRYPTION, 1.0_555507e9-85f8-4e41-96de-860b59f10bbe

Table 4: Platform Info

Data Point	Description	Example Value
CPU	CPU usage in past 5 minutes	fiveSecondsPercentage: 0.2000000, oneMinutePercentage: 0, fiveMinutesPercentage: 0
Memory	Memory usage	freeMemoryInBytes: 225854966384, usedMemoryInBytes: 17798281616, totalMemoryInBytes: 243653248000
Disk	Disk usage	freeGB: 21.237285, usedGB: 0.238805, totalGB: 21.476090

Data Point	Description	Example Value
Bandwidth	Bandwidth usage	receivedPktsPerSec: 3, receivedBytesPerSec: 212, transmittedPktsPerSec: 3, transmittedBytesPerSec: 399

Table 5: Feature Info

Data Point	Description	Example Value
Feature List	Enabled feature list	name: cluster status: enabled

Table 6: Cluster Info

Data Point	Description	Example Value
Cluster Info	Cluster information	clusterGroupName : ssp-cluster interfaceMode : spanned unitName : unit-3-3 unitState : SLAVE otherMembers : items : memberName : unit-2-1 memberState : MASTER memberSerialNum : FCH183771BA

Table 7: Failover Info

Data Point	Description	Example Value
Failover	Failover information	myRole: Primary, peerRole: Secondary, myState: active, peerState: standby, peerSerialNum: FCH183770EZ

Table 8: Login Info

Data Point	Description	Example Value
Login	Login history	loginTimes: 2 times in last 2 days, lastSuccessfulLogin: 12:25:36 PDT Mar 11 2019

ASA Telemetry Data Sample

Following is an example of the telemetry data that are sent from ASA in JSON format. When service manager receives this input, it aggregates the data from all ASAs and adds necessary headers/fields before sending to the SSE connector. The headers/fields include “version”, “metadata”, “payload” with “recordedAt”, “recordType”, “recordVersion”, and ASA telemetry data, "smartLicenseProductInstanceIdentifier", "smartLicenseVirtualAccountName", and alike.


```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
    "deviceInfo": {
        "deviceModel": "Cisco Adaptive Security Appliance",
        "serialNumber": "AANNNXXX",
        "systemUptime": 285,
        "udiProductIdentifier": "FPR9K-SM-36",
        "deploymentType": "Native",
        "securityContextMode": "Single"
    },
    "versions": {
        "items": [
            {
                "type": "asa_version",
                "version": "201.4(1)82"
```

```
            },
            {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
            }
        ]
    },
    "licenseActivated": {
        "items": [
            {
                "type": "Strong encryption",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",

                "count": 1
            },
            {
                "type": "Carrier",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "count": 1
            }
        ]
    },
    "CPUUsage": {
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0,
        "fiveMinutesPercentage": 0
    },
    "memoryUsage": {
        "freeMemoryInBytes": 99545662064,
        "usedMemoryInBytes": 20545378704,
        "totalMemoryInBytes": 120091040768
    },
    "diskUsage": {
        "freeGB": 21.237027,
        "usedGB": 0.239063,
        "totalGB": 21.476090
    },
    "bandwidthUsage": {
        "receivedPktsPerSec": 3,
        "receivedBytesPerSec": 268,
        "transmittedPktsPerSec": 4,
        "transmittedBytesPerSec": 461
    },
    "featureStatus": {
        "items": [
            {
                "name": "call-home",
                "status": "enabled"
            },
            {
                "name": "cluster",
                "status": "enabled"
            },
            {
                "name": "firewall_user_authentication",
                "status": "enabled"
            },
            {
                "name": "inspection-dns",
                "status": "enabled"
            },
            {
```

```
            "name": "inspection-esmtp",
            "status": "enabled"
        },
        {
            "name": "inspection-ftp",
            "status": "enabled"
        },
        {
            "name": "inspection-netbios",
            "status": "enabled"
        },
        {
            "name": "inspection-rsh",
            "status": "enabled"
        },
        {
            "name": "inspection-sip",
            "status": "enabled"
        },
        {
            "name": "inspection-sqlnet",
            "status": "enabled"
        },
        {
            "name": "inspection-sunrpc",
            "status": "enabled"
        },
        {
            "name": "inspection-tftp",
            "status": "enabled"
        },
        {
            "name": "inspection-xdmcp",
            "status": "enabled"
        },
        {
            "name": "logging-console",
            "status": "informational"
        },
        {
            "name": "management-mode",
            "status": "normal"
        },
        {
            "name": "sctp-engine",
            "status": "enabled"
        },
        {
            "name": "threat_detection_basic_threat",
            "status": "enabled"
        },
        {
            "name": "threat_detection_stat_access_list",
            "status": "enabled"
        },
        {
            "name": "webvpn-activex-relay",
            "status": "enabled"
        },
        {
            "name": "webvpn-dtls",
            "status": "enabled"
        }
    ]
```

```
    },
    "clusterInfo": {
        "clusterGroupName": "ssp-cluster",
        "interfaceMode": "spanned",
        "unitName": "unit-3-3",
        "unitState": "SLAVE",
        "otherMembers": {
            "items": [
                {
                    "memberName": "unit-2-1",
                    "memberState": "MASTER",
                    "memberSerialNum": "FCH183771BA"
                },
                {
                    "memberName": "unit-2-3",
                    "memberState": "SLAVE",
                    "memberSerialNum": "FLM1949C6JR"
                },
                {
                    "memberName": "unit-2-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-1",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                }
            ]
        }
    },
    "loginHistory": {
        "loginTimes": "1 times in last 1 days",
        "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
    }
}
```


Debug Telemetry Data

Before you begin

- Enable the telemetry service on ASA. See Enable or Disable Cisco Success Network , on page 2

Procedure

Step 1 To view the debug messages related to telemetry, enable the debug telemetry service using the following command in the privileged EXEC mode:

debug telemetry<*1-255*>

Example:

```
asa# debug telemetry ?
   <1-255>  Specify an optional debug level (default is 1)
```

Use the **no** form of the command to disable the debug telemetry service.

Step 2 To view the debug telemetry messages for the selected debug level, use the following command:

show debug telemetry

Example:

```
asa# show debug telemetry
debug telemetry  enabled at level 1

[telemetry_collect_device_info]: telemetry successfully collected device info
[telemetry_collect_versions]: telemetry successfully collected version info
[telemetry_collect_licenses]: no smart-lic entitlement in use
[telemetry_collect_cpu]: telemetry successfully collected cpu info
[telemetry_collect_memory]: telemetry successfully collected mem info
[telemetry_collect_disk_usage]: telemetry successfully collected disk info
[telemetry_collect_bandwidth_usage]: telemetry successfully collected bandwidth usage info
[telemetry_collect_enabled_feature_status]: telemetry successfully collected enabled feature
 info
[telemetry_collect_cluster_info]: telemetry successfully collected cluster info
[telemetry_collect_failover_info]: ha is not configured
[telemetry_get_user_login_hist]: telemetry successfully collected login history
[telemetry_collect_blocks]: telemetry successfully collected block info
[telemetry_collect_perfmon]: telemetry successfully collected perfmon stats
[telemetry_collect_resource_usage]: telemetry successfully collected res usage
[telemetry_collect_process_cpu_usage]: telemetry successfully collected res usage
[telemetry_collect_crashinfo]: telemetry successfully collected crashinfo
[telemetry_collect]: the serialized string is generated
[telemetry_collect]: successfully allocated mem for serialized string
[telemetry_history_add_record]: telemetry has a new history record: 16:23:29 PDT Oct 22
2019: Telemetry support on the blade: enabled
[telemetry_history_add_record]: telemetry has a new history record: 16:24:01 PDT Oct 22
2019: Telemetry support on the blade: disabled
```